Automating NIST Secure Software Development Framework (SSDF) with DigiCert Software Trust Manager

Introduction

The NIST Secure Software Development Framework (SSDF) Version 1.1 outlines fundamental practices for secure software development, aiming to reduce software vulnerabilities and their exploitation. Implementing these practices can be challenging due to the complexity and technical depth required.

Because these best practices can impact the efficiency of the software development lifecycle, automation is key to successful implementation. DigiCert Software Trust Manager automates many of the framework's best practices to avoid impact on the SDLC while at the same time provides an integrated, scalable infrastructure along with centralized security enforcement and visibility needed by the organization's security team.

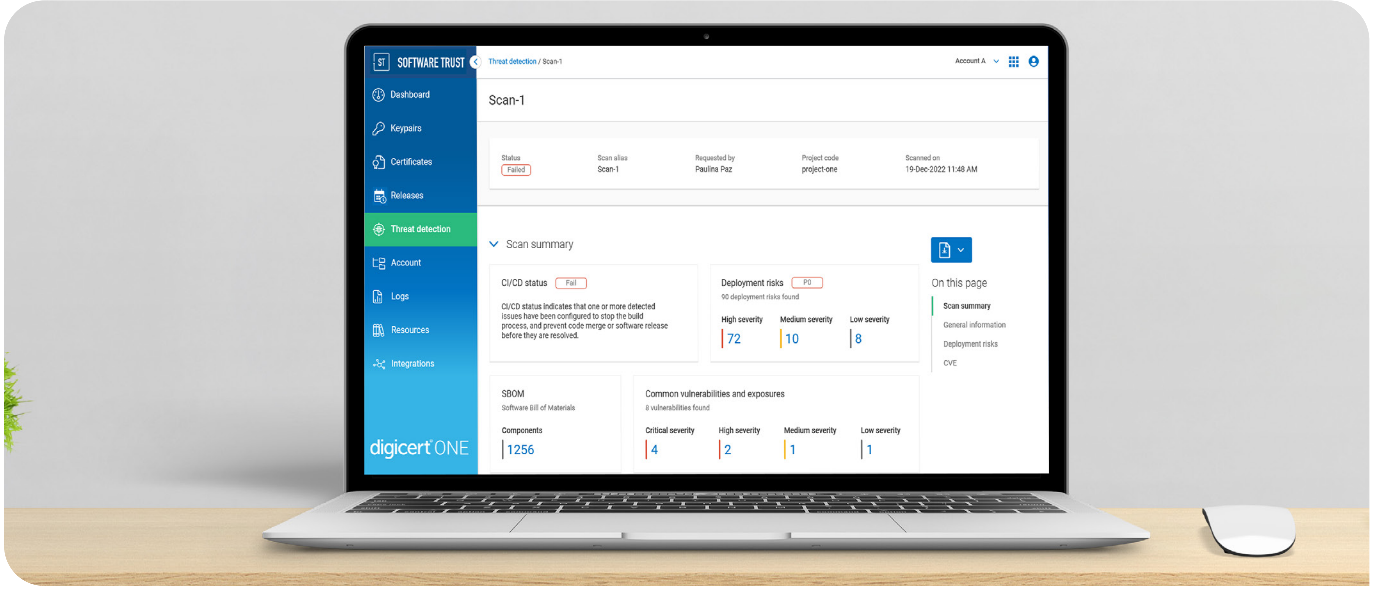
This paper outlines how the various capabilities of DigiCert Software Trust Manager can automate and enforce the NIST SSDF framework's best practices.

Overview of DigiCert Software Trust Manager

DigiCert Software Trust Manager is a comprehensive solution designed to enhance software security through malware, vulnerability and threat detection, software release management, code signing, certificate and cryptographic key management, and software bills of materials. Its capabilities align with the SSDF's goals, offering an integrated platform to secure software development processes.

Simplifying SSDF Implementation

The table below maps key features of DigiCert Software Trust Manager to the corresponding practices recommended by the NIST SSDF, demonstrating how the solution simplifies and automates the implementation of secure software development practices.



Scan-1

Status: Failed | Scan alias: Scan-1 | Requested by: Paulina Paz | Project code: project-one | Scanned on: 19-Dec-2022 11:48 AM

Scan summary

CI/CD status: Fail

CI/CD status indicates that one or more detected issues have been configured to stop the build process, and prevent code merge or software release before they are resolved.

Deployment risks: P0

90 deployment risks found

High severity	Medium severity	Low severity
72	10	8

SBOM

Software Bill of Materials

Components: 1256

Common vulnerabilities and exposures

8 vulnerabilities found

Critical severity	High severity	Medium severity	Low severity
4	2	1	1

NIST SSDF Best Practices

DigiCert Software Trust Manager capabilities. (The URLs direct to user documentation for more details)

Prepare the Organization (PO)		
PO.2: Implement Roles and Responsibilities	PO 2.1: Create roles and responsibilities of those involved in SDLC, including security roles, project managers, engineers. Implement and use tools to promote these roles and responsibilities.	The roles and custom roles capabilities enables teams to specify which users have authority to do things perform a code signing operation, approve the use of a code signing certificate, perform threat and malware scanning, or just have visibility into all security logs for compliance and audit requirements. These are customizable per software team/ project. The projects capability provides teams with a structured and collaborative environment to manage threat and malware scanning for a particular software project. The releases capability provides a means to specify the circumstances by which a code signing certificate may be used including which users and roles have access to it.
PO.3: Implement Supporting Toolchains	PO3.2: Follow recommended security practices to deploy and operate tool chains. PO 3.3: Configure tools to generate artifacts of their support of secure software development practices.	Software Trust Manager easily integrates with most CI/CD toolsets making it easy to incorporate into build pipelines without negatively impacting software developers' productivity. Software Trust Manager generates an irrefutable log of security actions taken for every software build. This can be obtained by the compliance and risk assessment teams. It automatically records approvals, code signing operations, files signed, and other important security events that occurred.
PO.5: Implement and maintain secure enviroments for software development	Use multi-factor authentication, network segmentation, enforce authentication, minimize direct human access to toolchains	Software Trust Manager integrates with customers' various identity management systems such as SAML and OpenID and supports MFA. Software Trust Manager prevents direct human access to secured code signing private keys, keeping them in secure FIPS 140-2 compliant storage at all times.

NIST SSDF Best Practices (continued...)

DigiCert Software Trust Manager capabilities. (The URLs direct to user documentation for more details)

Produce Well-Secured Software (PW)		
PW.1 Design Software Securely	PW1.1: Use forms of threat modeling and detection to identify risky aspects of the software. PW1.2: Track and maintain security requirements and decisions. PW1.3: Build in support for using standardized security features	Software Trust Manager provides a comprehensive threat, vulnerability, and malware scan comparing threat signatures to a database of over 25B known threats & vulnerabilities. This is performed for every release cycle. Known aspects about the threats (including severity) is presented to the development and security teams to help establish if the software should be released or not. In addition, code signing of the final executable can be automatically prevented should serious risks be discovered. Software Trust Manager automatically records all outcomes from threat scanning. Software Trust Manager integrates into SDLC build pipelines to automatically perform and record security scans and actions.
PW.4 Verify third party software complies with security requirements		Software Trust Manager integrates with FOSSA open-source scanning tool to ensure that unsafe third party is flagged. In addition, by scanning final binaries as well, Software Trust Manager scans all software components in the final executable and thus will detect potentially unsafe ones.

Respond to Vulnerabilities (RV)		
RV.1 Prepare for Vulnerability Reports	RV.1.1: Gather information from software acquirers, users, and public sources on potential vulnerabilities.	Software Trust manager leverages multiple sources of threat, vulnerability and malware databases including public sources.
RV.2 Remediate Vulnerabilities	RV:2.1: Analyze each vulnerability to gather sufficient information about risk.	Software Trust Manager provides information related to severity and recommended courses of action.

Conclusion

DigiCert Software Trust Manager automates and significantly simplifies the implementation of the NIST SSDF by providing a scalable and enterprise-hardened software development security infrastructure that can be easily deployed across all size of companies. By leveraging DigiCert Software Trust Manager, organizations can enhance their software development security posture, reduce vulnerabilities, and comply with industry standards efficiently.